



[Subscribe](#) (Full Service) [Register](#) (Limited Service, Free) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

"relying participant service" and array and "relying customer interface"



[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Terms used **relying participant service** and **array** and **relying customer interface** and **digest** and **digital signature**

Found 1,104 of 157,873

Sort results by

Display results

[Save results to a Binder](#)

[Search Tips](#)

☐ [Open results in a new window](#)

[Try an Advanced Search](#)

[Try this search in The ACM Guide](#)

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale ☐ ☐ ☐ ☐ ☐

- 1 [The SecureRing group communication system](#)  
Kim Potter Kihlstrom, L. E. Moser, P. M. Melliar-Smith  
November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4

Full text available: [pdf\(1.03 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

- 2 [A semantics for web services authentication](#)  
Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon  
January 2004 **ACM SIGPLAN Notices , Proceedings of the 31st ACM SIGPLAN-SIGACT symposium on Principles of programming languages**, Volume 39 Issue 1

Full text available: [pdf\(234.06 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

- 3 [Digital signatures: can they be accepted as legal signatures in EDI?](#)  
Patrick W. Brown  
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Full text available: [pdf\(609.34 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

- 4 [Flexible control of downloaded executable content](#)  
Trent Jaeger, Atul Prakash, Jochen Liedtke, Nayeem Islam  
May 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 2

Full text available: [pdf\(297.79 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

- 5 [Session 4: Web service applications: Authenticating distributed data using Web services and XML signatures](#)  
Daniel J. Polivy, Roberto Tamassia  
November 2002 **Proceedings of the 2002 ACM workshop on XML security**

Full text available: [pdf\(164.09 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

- 6 [Wireless and mobility: Evaluation of two security schemes for mobile agents](#)  
Igor Sobrado  
April 2001 **ACM SIGCOMM Computer Communication Review**, Volume 31 Issue 2 supplement

Full text available: [pdf\(2.10 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

7 Hop integrity in computer networks

Mohamed G. Gouda, E. N. (Mootaz) Elnozahy, Chin-Tser Huang, Tommy M. McGuire  
June 2002 **IEEE/ACM Transactions on Networking (TON)**, Volume 10 Issue 3

Full text available: [pdf\(366.26 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

8 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov  
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Full text available: [pdf\(1.63 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

9 The design and implementation of a private message service for mobile computers

David A. Cooper, Kenneth P. Birman  
March 1995 **Wireless Networks**, Volume 1 Issue 3

Full text available: [pdf\(1.35 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

10 Authentication in the Taos operating system

Edward Wobber, Martín Abadi, Michael Burrows, Butler Lampson  
February 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 1

Full text available: [pdf\(1.88 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

11 SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu  
August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications**, Volume 34 Issue 4

Full text available: [pdf\(236.82 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

12 A secure and private system for subscription-based remote services

Pino Persiano, Ivan Visconti  
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4

Full text available: [pdf\(241.65 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

13 Constructing replicated systems using processors with point-to-point communication links

P. D. Ezhilchelvan, S. K. Shrivastava, A. Tully  
April 1989 **ACM SIGARCH Computer Architecture News , Proceedings of the 16th annual international symposium on Computer architecture**, Volume 17 Issue 3

Full text available: [pdf\(948.34 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

14 Anonymous E-prescriptions

Giuseppe Ateniese, Breno de Medeiros  
November 2002 **Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society**

Full text available: [pdf\(304.10 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

15 Revising old friends: Separating agreement from execution for byzantine fault tolerant services

Jian Yin, Jean-Philippe Martin, Arun Venkataramani, Lorenzo Alvisi, Mike Dahlin

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Full text available:  [pdf\(355.08 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

16 Security: Geometric distortion-resilient image hashing system and its application scalability

Chao-Yong Hsu, Chun-Shien Lu


September 2004 **Proceedings of the 2004 multimedia and security workshop on Multimedia and security**

Full text available:  [pdf\(1.07 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

17 Protecting digital media content

Nasir Memon, Ping Wah Wong

July 1998 **Communications of the ACM**, Volume 41 Issue 7

Full text available:  [pdf\(1.02 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#), [review](#)

18 Exploration for advanced SoC design: An HMAC processor with integrated SHA-1 and MD5 algorithms

Mao-Yin Wang, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu

January 2004 **Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04 , Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04**

Full text available:  [pdf\(60.57 KB\)](#)  Additional Information: [full citation](#), [abstract](#), [references](#), [Publisher Site](#)

19 Java resources for computer science instruction

Joseph Bergin, Thomas L. Naps, Constance G. Bland, Stephen J. Hartley, Mark A. Holliday, Pamela B. Lawhead, John Lewis, Myles F. McNally, Christopher H. Nevison, Cheng Ng, George J. Pothering, Tommi Teräsvirta

December 1998 **Working Group reports of the 3rd annual SIGCSE/SIGCUE ITiCSE conference on Integrating technology into computer science education**

Full text available:  [pdf\(107.98 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

20 Java resources for computer science instruction

Joseph Bergin, Thomas L. Naps, Constance G. Bland, Stephen J. Hartley, Mark A. Holliday, Pamela B. Lawhead, John Lewis, Myles F. McNally, Christopher H. Nevison, Cheng Ng, George J. Pothering, Tommi Teräsvirta

December 1998 **ACM SIGCSE Bulletin**, Volume 30 Issue 4

Full text available:  [pdf\(2.29 MB\)](#) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

» Search Results

[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "'((digital signature' and array)&lt;in&gt;metadata)'"

☒ e-mail

Your search matched 13 of 1194402 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.» [View Session History](#)» [New Search](#)

Modify Search

» Key

((digital signature' and array)&lt;in&gt;metadata)



IEEE JNL IEEE Journal or Magazine

☐ Check to search only within this results set

IEEE JNL IEE Journal or Magazine

Display Format: ☐ Citation ☒ Citation & Abstract

IEEE CNF IEEE Conference Proceeding

Select Article Information

IEEE CNF IEE Conference Proceeding

**1. Design of a novel two-element phased array for wireless applications**McNeil, D.; Denidni, T.A.; Delisle, G.Y.;  
Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference  
Volume 3, 4-7 May 2003 Page(s):1429 - 1432 vol.3**Summary:** In this contribution, the design of a novel two-element phased array for miti;  
interference effects in digital mobile communications is presented. This new antenna s;  
for applications at the handset level. To control the phase.....[AbstractPlus](#) | Full Text: [PDF\(329 KB\)](#) IEEE CNF**2. An efficient implementation of the digital signature algorithm**Kitsos, P.; Sklavos, N.; Koufopavlou, O.;  
Electronics, Circuits and Systems, 2002. 9th International Conference on  
Volume 3, 15-18 Sept. 2002 Page(s):1151 - 1154 vol.3**Summary:** Digital signature schemes are commonly used as primitives in cryptographi  
provide other services including entity authentication, authenticated key transport, and  
agreement. A VLSI implementation of the digital signa.....[AbstractPlus](#) | Full Text: [PDF\(330 KB\)](#) IEEE CNF**3. Design and implementation of an RSA public-key cryptosystem**Jyh-Huei Guo; Chin-Liang Wang; Hung-Chih Hu;  
Circuits and Systems, 1999. ISCAS '99. Proceedings of the 1999 IEEE International Sy  
Volume 1, 30 May-2 June 1999 Page(s):504 - 507 vol.1**Summary:** This paper presents a new bit-serial systolic array for realizing a modified M  
algorithm for modular multiplication. The proposed array is highly regular, modular, and  
to be implemented using VLSI techniques. It does not inv.....[AbstractPlus](#) | Full Text: [PDF\(324 KB\)](#) IEEE CNF**4. FPGA implementation of GF (P/sup m/) exponentiation for digital signature and a scheme**Fang Han; JianPeng Chu; ZongSheng Lai; Tao Tao; ChengShi Li; XinBing Li; JianJun '  
Solid-State and Integrated Circuits Technology, 2004. Proceedings. 7th International C  
Volume 3, 18-21 Oct. 2004 Page(s):2039 - 2042 vol.3**Summary:** This contribution describes a field programmable gate array (FPGA) implem  
exponentiation over GF (P/sup m/), the arithmetic architecture of which is based on the  
transform (FNT). The main applications of the processor are dig.....[AbstractPlus](#) | Full Text: [PDF\(152 KB\)](#) IEEE CNF**5. Research on computing IP core for the digital signature algorithm**

Jianpeng Chu; Yongsheng Xu; Xiaojin Li; Zongsheng Lai;  
ASIC, 2003. Proceedings. 5th International Conference on  
Volume 2, 21-24 Oct. 2003 Page(s):1329 - 1331 Vol.2

**Summary:** Polynomial multiplication with big integer coefficients over finite field is frequent in some digital signature algorithms, in which this kind of calculation is the most time consuming realized by software. This paper presents a new method.....

[AbstractPlus](#) | Full Text: [PDF\(221 KB\)](#) IEEE CNF



#### 6. Digital watermarking through quasi m-arrays

Yeh, C.H.; Kuo, C.J.;  
Signal Processing Systems, 1999. SiPS 99. 1999 IEEE Workshop on  
20-22 Oct. 1999 Page(s):456 - 461

**Summary:** Watermark is an important protection and identification technique that allows to be hidden in the multimedia information such as audio, image, video, or text and has to protect digital signal against illegal reproduction.....

[AbstractPlus](#) | Full Text: [PDF\(172 KB\)](#) IEEE CNF



#### 7. Digital watermarking through quasi m-arrays

Yeh, C.H.; Kuo, C.J.;  
Industrial Electronics Society, 1999. IECON '99 Proceedings. The 25th Annual Conference  
Volume 1, 29 Nov.-3 Dec. 1999 Page(s):459 - 461 vol.1

**Summary:** Watermarking is an important protection and identification technique that allows to be hidden in the multimedia information such as audio, image, video, or text and has to be developed to protect digital signals against illegal reproduction.....

[AbstractPlus](#) | Full Text: [PDF\(196 KB\)](#) IEEE CNF



#### 8. A prototype test system for massively-parallel electrical testing of high density interconnect substrates

Newman, K.E.; Keezer, D.C.;  
Advanced Packaging Materials, 1998. Proceedings. 1998 4th International Symposium  
15-18 March 1998 Page(s):138

**Summary:** Summary form only given. Conventional tests for electrical interconnections on substrates utilize one or more moving probes to measure net capacitance and/or resistance nodes. These methods provide adequate fault coverage for high density interconnect.....

[AbstractPlus](#) | Full Text: [PDF\(80 KB\)](#) IEEE CNF



#### 9. A hardware implementation of MD4-family hash algorithms

Dominikus, S.;  
Electronics, Circuits and Systems, 2002. 9th International Conference on  
Volume 3, 15-18 Sept. 2002 Page(s):1143 - 1146 vol.3

**Summary:** This article presents the design of an integrated circuit which is able to perform different hash algorithms of the MD4 family. Hash algorithms are used for digital signature data integrity, message authentication, and other cryptographic.....

[AbstractPlus](#) | Full Text: [PDF\(360 KB\)](#) IEEE CNF



#### 10. Publicly detectable techniques for the protection of virtual components

Gang Qu;  
Design Automation Conference, 2001. Proceedings  
2001 Page(s):474 - 479

**Summary:** Highlighted with the newly released intellectual property (IP) protection while the Alliance, the protection of virtual components (VCs) has received a large amount of attention. Digital signature is one of the most promising solutions.....

[AbstractPlus](#) | Full Text: [PDF\(748 KB\)](#) IEEE CNF






#### 11. Proceedings of the Twenty-First National Radio Science Conference (IEEE Cat. N)

National Radio Science Conference, 2004. NRSC 2004. Proceedings of the Twenty-First  
16-18 March 2004

**Summary:** Not available.....

Full Text: [PDF\(195 KB\)](#) IEEE CNF

-  **12. Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function**  
Michail, H.E.; Kakarountas, A.P.; Milidonis, A.; Goutis, C.E.;  
Electronics, Circuits and Systems, 2004. ICECS 2004. Proceedings of the 2004 11th IEEE Conference on  
13-15 Dec. 2004 Page(s):567 - 570  
**Summary:** In this paper, an efficient implementation, in terms of performance, of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function is presented. This implementation is used for message authentication in combination with a shared secret key.....  
[AbstractPlus](#) | Full Text: [PDF\(557 KB\)](#) IEEE CNF
-  **13. On the hardware design of an elliptic curve cryptosystem**  
Morales-Sandoval, M.; Feregrino-Urbe, C.;  
Computer Science, 2004. ENC 2004. Proceedings of the Fifth Mexican International Conference on  
2004 Page(s):64 - 70  
**Summary:** We present a hardware architecture for an elliptic curve cryptography system. The system implements three basic cryptographic schemes: DH key generation, encryption and digital signature. The hardware architecture is described by using hardware description languages,.....  
[AbstractPlus](#) | Full Text: [PDF\(279 KB\)](#) IEEE CNF
- 

Indexed by  


[Help](#) [Contact Us](#) [Privacy & Policy](#)

© Copyright 2005 IEEE ...